Practical Post-quantum Password-Authenticated Key Exchange Based-on Module-Lattice

Peixin Ren and Xiaozhuo Gu*

SKLOIS, Institute of Information Engineering, CAS, Beijing, China
School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
{renpeixin, guxiaozhuo}@iie.ac.cn

Abstract. Password-authenticated key exchange (PAKE) is a neat technology that can establish secure remote communications between the client and the server, especially with the preponderance (importance/necessity) of amplifying a memorable password into a strong session key. However, the arrival of the quantum computing era has brought new challenges to traditional PAKE protocols. Thus, designing an efficient post-quantum PAKE scheme becomes an open research question. In this paper, we construct a quantum-safe PAKE protocol which is a horizontal extension of the PAK protocol [22] in the field of module lattice. Subsequently, we accompany our proposed protocol with a rigorous security proof in the Bellare-Pointcheval-Rogaway (BPR) model with two adaptions: applying the CDF-Zipf model to characterize the ability of the adversary and using the pairing with errors (PWE) assumption to simplify the proof. Taking the flexibility of the module learning with errors (MLWE) problem, we elaborately select 3 parameter sets to meet different application scenarios (e.g., classical/quantum-safe Transport Layer Security (TLS), resource-constrained Internet of Things (IoT) devices). Specifically, our Recommended implementation achieves 177-bit post-quantum security with a generous margin to cope with later improvement in cryptanalysis. The performance results indicate that our MLWE-PAKE is quite practical: compared with the latest Yang-PAK, our Recommended-PAK reduces the communication cost and the running time by 36.8% and 13.8%, respectively.

Keywords: Password-authenticated key exchange · Module learning with errors · Post-quantum · Lattice-based.

1 Introduction

Passwords have several advantages of being human-memorable, avoiding expensive computation of public key infrastructure (PKI) to distribute client certificates, and preventing dedicated hardware for storing secret keys. Thus, passwords constitute the prevalent and irreplaceable authentication approach to identify human users [31, 26], especially in the proliferation of mobile devices.

* Corresponding author: guxiaozhuo@iie.ac.cn.